

Personal Health Record over Encrypted Data Using Cloud Service

Dinesh Soni¹, Dr. Lakshmi JVN²

¹Master of Computer Application, ²Associate Professor,

^{1,2}Jain University, Bengaluru, Karnataka, India

ABSTRACT

CBPHR- Cloud Based Personal Health Record systems are used for storage and management of patient records. Cloud computing provides real time health care data in a convenient and cost effective manner. Due to the lack of visibility in cloud platform, the users are always concerned with data privacy and security. This is the main obstacle in widely adopting CBPHR systems in health care sector. The paper is discussing a cloud based patient health record management scheme which is highly secured. In this approach, indexes are encrypted under different symmetric keys and also the encrypted data indexes from various data providers can be merge by cloud without knowing the index content. It also provides efficient and privacy preserving query processing using a single data query submitted by the data user. Encrypted data will be processed by cloud from all related data providers without knowing its query content.

KEYWORDS: CBPHR, Access Controls, Encryption, Trapdoor Key, File Key

How to cite this paper: Dinesh Soni | Dr. Lakshmi JVN "Personal Health Record over Encrypted Data Using Cloud Service" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-4, June 2021, pp.292-294, URL: www.ijtsrd.com/papers/ijtsrd41230.pdf



IJTSRD41230

Copyright © 2021 by author(s) and International Journal of Trend in Scientific Research and Development Journal. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0) (<http://creativecommons.org/licenses/by/4.0>)



I. INTRODUCTION

There has been a massive adoption of cloud computing in the generation, storage, manipulation and sharing of data. The same happens in healthcare sector. Cloud computing has benefits for both healthcare professionals and patients. Usage of cloud solutions can cut down operational expenses and is also very convenient for the users because of the accessibility. [6] Cloud Based Personal Health Record systems should be designed in such a way where the health records should be stored and processed in a highly secured manner. Patient care should be given utter importance and should be improved with time. Cloud computing provides personalized care for the patients as they are provided with personal spaces to view and understand their health reports any time and from anywhere. Security and privacy of healthcare documents which are always considered sensitive is the problem in adopting cloud computing for the storage and processing of such data. [1]

Healthcare data management system involves consultation and prescription files, diagnosis reports and other digital media like x-ray and scanning reports. All these data can be uploaded and accessed by the users of the cloud platform. This multi user environment can be vulnerable with an increase in usage and popularity. In this paper, a Cloud Based Personal Health Record (CBPHR) system is proposed that uses encryption technique to protect the privacy of the uploaded data. In this approach, authentication and authorization of cloud users are given great importance. In section II, existing system and in section III, proposed system

is discussed. In section IV, the architecture diagram is presented. In section V, the paper is concluded with future recommendations.

II. Existing System

A Cloud Based Patient Health Record (CBPHR) system should always be designed in such a way so that it can perform the expected operations in a relevant and feasible manner to all the users.[4] The users of healthcare system comprises of hospital staff members like doctors, nurses, lab technicians, microbiologists and even the receptionists. All these people can be categorized as data owners who are the sources of clinical data. Other than healthcare professionals, patients are the most important part of a healthcare management system as they are the primary data users. While the security and privacy of the data users are of great importance, still most of the healthcare management systems are not sufficiently secured. [5]

Some of the Personal Health Record (PHR) systems are deployed on cloud while others makes use of traditional approach. [2] Encryption is a technique through which we can hide the true sense of our information is somewhat common in CBPHR systems. But still many of those users can download the files without proper authentication. Storing a data securely is not sufficient for a secure system but also the access to the data should be restricted. This may cause a disagreement among the users because the process is tiring and time consuming. Most CBPHR systems are openly accessible to people and anybody can create a user

account.[7] This is a disadvantage because anybody with a little knowledge about a patient can easily create a fake account and access that person's personal data.

Creating an ideal CBPHR system requires processes like access control and encryption. Here, the access control strategy should not be limited to data uploading or downloading but also in the creation of user accounts. [3]

III. Proposed System

The proposed system is a Cloud Based Personal Health Record (CBPHR) system that integrates the concepts of access control and encryption. In this approach, the entire patient documents are uploaded in encrypted format. A trapdoor key is used by the data provider to upload the documents. The same way the data users can access the reports and other documents through the platform using a file key. Here, trapdoor key acts as the encryption key and file key acts as the decryption key. The proposed method gives great importance to access control. The data providers and data users require permission from cloud server to access the cloud platform.

The system involves 4 modules namely, Data Owner, Data User, Authority, Attributor and Cloud Server. Data Owner can be a doctor or hospital staff who creates data. Once a doctor registers an account, the cloud server has to authorize the particular person to login. The data owner can upload

patient files to the system using a trapdoor key provided by the admin or authority module. A data owner can view and edit their patient details accordingly. The same way, the data user can search for their own reports and can also download it using a file key provided by the attributor module. The data user account creation happens the same way as the data owner. They should also be authenticated by the cloud server before accessing the data. If the data user enters the wrong file key, the application suspects this user to be an attacker. The main goal of the approach is to secure the system against chosen-keyword attack. Based on the search file, they can be able to request the key from the attributor. Once they received the key from the attributor, the data user can download the file. Cloud server is the authorized module to grant permission, monitor all the patient details, Clinical report details, attacker details and result analysis of a particular system. The system is really much secured because it is completely encrypted and the privileges are being taken care of. [8]

IV. System Architecture

The below figure [fig 1] is showing the system architecture. It is a pictorial representation of the entire cloud based patient health record system. In this, all the modules and their interdependencies are demonstrated. The encryption, decryption and authorization processes are also displayed in detail.

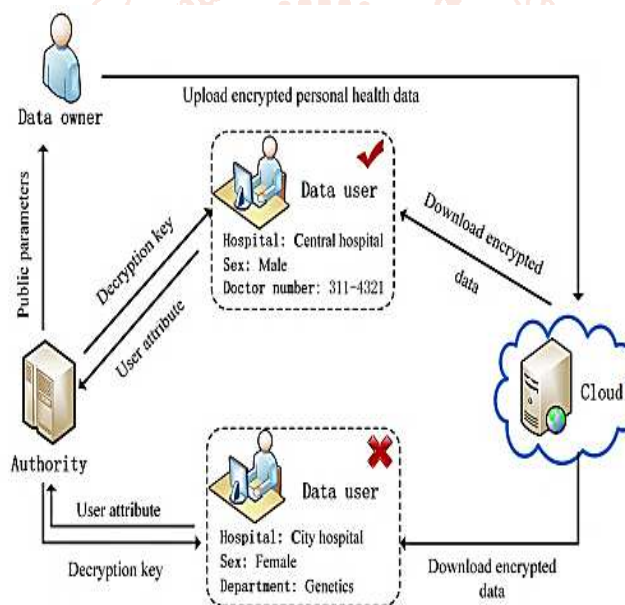


Fig 1: System Architecture

V. Conclusion and Future Enhancements

The paper proposes an efficient and privacy preserving technique where data and data indexes are encrypted using different symmetric keys and also the encrypted data from multiple providers can merge in the cloud without knowing its content. This is a cloud based patient health record system with secured data storage and manipulation features. This is a system that is helpful to the patients because of its usability and simplicity. The proposed approach is also giving importance to the authorization and authentication processes.

As a future enhancement, we can transform clinical data into knowledge for better patient care. Supervised Learning concept in Machine learning and Artificial Intelligence technology can be used for analyzing and training the system based on existing records like clinical data, genetical data and medical history. This is helpful for predicting any

possible disease. This kind of systems can also monitor the patient in real time. Here, wireless patient monitoring devices like heart rate monitor, pulse oximeter, sphygmomanometer etc. can be connected to the database or server to store and monitor the patient's body changes. This can benefit both the technology and healthcare industry to save the human life.

VI. References

- [1] M. P. Radhini, P. Ananthaprabha, P. Parthasarathi, Secure Sharing of Medical Records Using Cryptographic Methods in Cloud, International Journal of Computer Science and Mobile Computing, Vol. 3, Issue. 4, April 2014, pg. 514 – 521
- [2] Ismail Keshta, Ammar Odeh, , Security and privacy of electronic health records: Concerns and challenges, Egyptian Informatics Journal, 2020, ISSN 1110-8665

- [3] Fernández-Alemán JL, Señor IC, Lozoya PÁ, Toval A. Security and privacy in electronic health records: a systematic literature review. J Biomed Inform. 2013 Jun; 46(3): 541-62. doi: 10.1016/j.jbi.2012.12.003. Epub 2013 Jan 8. PMID: 23305810.
- [4] Pradeep Deshmukh, , Design of cloud security in the EHR for Indian healthcare services, Journal of King Saud University - Computer and Information Sciences, Volume 29, Issue 3, 2017, Pages 281-287, ISSN 1319-1578
- [5] Samuel, Victoria & Adewumi, Adewole & Dada, Benjamin & Omeregbe, Nicholas & Misra, Sanjay & Odusami, Modupe. (2019). Design and Development of a Cloud-Based Electronic Medical Records (EMR) System. 10.1007/978-981-13-6351-1_3.
- [6] Adebayo, Abayomi-Alli & Ikuomola, Aderonke & Robert, Ifeoluwa & Abayomi-Alli, Olusola. (2014). An Enterprise Cloud-Based Electronic Health Records System. 2. 21-36.
- [7] Pradeep Deshmukh, Design of cloud security in the EHR for Indian healthcare services, Journal of King Saud University - Computer and Information Sciences, Volume 29, Issue 3, 2017, Pages 281-287, ISSN 1319-1578.
- [8] Jesús Romero, Pablo López, José Luis Vázquez Noguera, Cristian Cappelletti, Diego P. Pinto-Roa and Cynthia Villalba , INTEGRATED, RELIABLE AND CLOUD-BASED PERSONAL HEALTH RECORD: A SCOPING REVIEW, Health Informatics - An International Journal (HIJ) Vol. 5, No. 2/3, August 2016.

